

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor: : **Haruo MORITOMO, et al.**  
Filed : **Concurrently herewith**  
For : **A SYSTEM, METHOD AND DEVICE....**  
Serial No. : **Concurrently herewith**

October 16, 2003

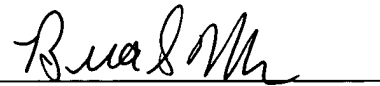
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**PRIORITY CLAIM AND**  
**SUBMISSION OF PRIORITY DOCUMENT**

S I R:

Applicant hereby claims priority under 35 USC 119 from **Japanese** patent application number **2002-301317** filed **October 16, 2002**, a copy of which is enclosed.

Respectfully submitted,



Brian S. Myers  
Reg. No. 46,947

Katten Muchin Zavis Rosenman  
575 Madison Avenue  
New York, NY 10022-2585  
(212) 940-8800  
Docket No.: FUJ 20.560

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年10月16日

出 願 番 号

Application Number:

特願2002-301317

[ ST.10/C ]:

[ JP 2002-301317 ]

出 願 人

Applicant(s):

富士通株式会社

2003年 4月 8日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

太田 信一郎

出証番号 出証特2003-3024403

【書類名】 特許願

【整理番号】 0251760

【提出日】 平成14年10月16日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00  
H04K 1/00

【発明の名称】 暗号通信を行うノード装置、暗号通信システムおよび方法

【請求項の数】 5

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 森友 春男

【発明者】

【住所又は居所】 神奈川県横浜市港北区新横浜3丁目9番18号 富士通コミュニケーション・システムズ株式会社内

【氏名】 田代 泰章

【発明者】

【住所又は居所】 神奈川県横浜市港北区新横浜3丁目9番18号 富士通コミュニケーション・システムズ株式会社内

【氏名】 谷口 明彦

【発明者】

【住所又は居所】 神奈川県横浜市港北区新横浜3丁目9番18号 富士通コミュニケーション・システムズ株式会社内

【氏名】 白井 信雄

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100108187

【弁理士】

【氏名又は名称】 横山 淳一

【電話番号】 044-754-3035

【手数料の表示】

【予納台帳番号】 011280

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0017694

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号通信を行うノード装置、暗号通信システムおよび方法

【特許請求の範囲】

【請求項 1】

1 つ以上のノード装置との間に第 1 の暗号トンネルをそれぞれ設定可能なノード装置において、

パケットを受信し、予め設定された暗号トンネルを介した経路にパケットを送出する手段と、

該経路を使用するパケットのトラヒック量が第 1 のいき値を超えたときに、該経路の終点となるノード装置との間に第 2 の暗号トンネルを構築する手段を備えることを特徴とするノード装置。

【請求項 2】

請求項 1 記載において、

前記第 2 の暗号トンネルのトラヒック量が第 2 のいき値を下回ったときに、前記第 2 の暗号トンネルから前記第 1 の暗号トンネルに切り換えることを特徴とするノード装置。

【請求項 3】

請求項 1 記載において、

前記第 1 の暗号トンネルから前記第 2 の暗号トンネルに切り換える処理を行うための切替え要求を示す情報を含む手段を備えることを特徴とするノード装置。

【請求項 4】

請求項 1 記載において、

前記第 1 の暗号トンネルをそれぞれ接続する前記すくなくとも 1 つのノード装置および前記経路の終点となるノード装置を有することを特徴とする暗号通信システム。

【請求項 5】

パケットを受信し、第 1 の経路に暗号化したパケットを送出するステップと

該第 1 の経路を使用して転送するパケットのトラヒック量が第 1 のいき値を超

えたときに、前記経路の終点となるノード装置との間に暗号トンネルを構築するステップを備えることを特徴とする暗号通信を行う方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、パケットを暗号処理し、暗号通信を行う通信方法、暗号通信を行う暗号通信システム、暗号通信を行うノード装置に関する。

【0002】

【従来の技術】

複数の拠点間との間をインターネットまたは専用／公衆回線を介して暗号通信を行うときには、IPsec (Internet Protocol security) 等のプロトコルに準拠して送信側で暗号化、受信側で復号化処理を行っていた。また、双方向通信においては、逆方向通信も同様な処理を行っていた。

【0003】

例えば、任意の2つ拠点の暗号通信を行う場合、第1の方法として、IPsecを使用したトンネルを介した仮想閉域網を構築する。そして、そのトンネルは、通常、その拠点間に構築されることが知られている。（例えば、特許文献1を参照）

また、第2の方法として、2つの拠点間に中継となる1つ以上の中継ノード（例えばルータ）を設け、例えば、第1の拠点と中継ノード（中継点とも呼ぶ。）、この中継ノードと第2の拠点との間にそれぞれトンネルを構築する方法が考えられる。

【0004】

前記第1の方法では、各拠点間にそれぞれトンネルを構築するため、必要とされるトンネル数は約拠点数の二乗に比例して増える。例えば、2拠点間では、1つのトンネルだが、5つの拠点（ $N=5$ ）のネットワークでは、 $N(N-1)/2=10$ のトンネルが必要である。また、100拠点間での通信では、 $100*99/2=4950$ のトンネルが必要である。

【0005】

したがって、各拠点とは他の全ての通信拠点とトンネルを構築（設定）するとすれば、トンネルの構築には拠点すべてに関する I P s e c 情報を管理・設定する必要がある。

#### 【 0 0 0 6 】

前記第 2 の方法では、拠点間を直結する I P s e c トンネルを構築せずに中継ノード（例えば、ルータ）を介して、2 つ以上の I P s e c トンネルを介して暗号通信を行う。自転車の車輪に例えると、中継ノードがハブに相当し、拠点がスポークの末端に接続される形態に対応させて考えることができる。なお、中継ノードは 2 つ以上あってもよいし、並列または直列に接続してもよい。

#### 【 0 0 0 7 】

これらトンネルの構築形態は異なるものの、各のトンネルの設定方法は同様である。

#### 【 0 0 0 8 】

図 1 は、中継ノードを設けたハブアンドスポークによる暗号通信の例を説明する図である。

#### 【 0 0 0 9 】

図中、例えば、端末 1 1 と端末 3 1 との間で暗号通信を行う場合を考える。

#### 【 0 0 1 0 】

端末 1 1 から端末 3 1 へのパケットを受信した拠点 1 のルータ 1 は、設定されたポリシーに従ってそのパケットを暗号化し、中継ノードのルータ 2 に送出する。ルータ 2 では、暗号化されたパケットを一旦復号化し、再度、暗号化して拠点 2 へ転送する。拠点 2 ではルータ 3 がそのパケットを復号化し端末 3 1 に転送する。このように暗号通信を行うことができる。

#### 【 0 0 1 1 】

1 つのトンネルを設定するタイミングは、暗号化対象 I P パケット受信時に、宛先拠点への暗号トンネルが存在しない場合に初めて構築する方式と、暗号化対象 I P パケット受信前に、暗号トンネルを構築しておく方式がある。

#### 【 0 0 1 2 】

通常、中継ノード方式（ハブアンドスポーク方式）では、前もって、中継ノ

ードと各拠点間を暗号トンネルにより接続することが好ましい。しかしながら、ダイナミックに前記暗号化トンネルを接続してもよい。

【0013】

【特許文献1】

特開 2 0 0 2 - 4 4 1 4 1 （例えば、図 2）

【0014】

【発明が解決しようとする課題】

拠点間をそれぞれ直接接続する暗号トンネルを構築（設定）する場合には、暗号通信を行う全ての拠点に設置されるノード（ルータ等）に、暗号トンネルの設定に関する情報を格納したデータベース、いわゆる SAD（Security Association Database）が必要である。SADに基づき構築される暗号トンネルが使用するリソースは暗号トンネルの数に比例し、かつ、使用しない暗号トンネルについてもリソースを占有することになる。すなわち、暗号通信が行われていないトンネルは、リソースを浪費していることになってしまう。また、暗号トンネルの設定（接続）が完了するまでパケット転送を開始できないという問題もあった。

【0015】

また、中継ノードにおいて、暗号トンネルを終端（暗号化パケットを復号化）し、中継ノードから第2の拠点へ再度暗号化して暗号化パケットを送信することになる。この暗号化および復号化の処理はノード装置にとって負荷の大きい処理であり、多量の暗号通信トラヒックを処理するためには高性能のノード装置を配置する必要がある。

【0016】

一方、暗号化対象 IP パケット受信をトリガに暗号トンネルを構築するには、複数メッセージケンスのやり取りが行われ、暗号トンネルの設定完了までには、後続暗号化対象 IP パケットを廃棄、もしくは待ち合わせすることになり、ネットワーク内の暗号通信のレスポンスが低下することになる。

【0017】

本発明は、暗号通信に使用されるトンネルに関するリソースを合理的に割り当



てることを目的とする。

【 0 0 1 8 】

【課題を解決するための手段】

本発明のノード装置は、1つ以上のノード装置との間に第1の暗号トンネルをそれぞれ設定可能なノード装置において、パケットを受信し、予め設定された暗号トンネルを介した経路にパケットを送出する手段と、該経路を使用するパケットのトラヒック量が第1のいき値を超えたときに、該経路の終点となるノード装置との間に第2の暗号トンネルを構築する手段を備えることを特徴とする。

【 0 0 1 9 】

本発明によれば、暗号化パケットのトラヒック量に応じて第2の暗号トンネルを構築することができ、暗号トンネルに関するリソースを合理的に割り当てることができる。

【 0 0 2 0 】

また、本発明のノード装置は、前記第2の暗号トンネルのトラヒック量が第2のいき値を下回ったときに、前記第2の暗号トンネルから前記第1の暗号トンネルに切り換えることを特徴とする。

【 0 0 2 1 】

また、本発明のノード装置は、前記第1の暗号トンネルから前記第2の暗号トンネルに切り換える処理を行うための切替え要求を示す情報を含む手段を備えることを特徴とする。

【 0 0 2 2 】

また、本発明の暗号通信システムは、すくなくとも1つ以上のその他ノード装置との間に第1の暗号トンネルをそれぞれ接続する前記ノード装置および前記ルートの終点となるノード装置を有することを特徴とする。

【 0 0 2 3 】

また、本発明の暗号通信システムは、また、前記第1の暗号トンネルをそれぞれ接続する前記すくなくとも1つのノード装置および前記経路の終点となるノード装置を有することを特徴とする。

【 0 0 2 4 】

また、本発明の暗号通信を行う方法は、パケットを受信し、デフォルトルートに暗号化したパケットを送出するステップと、

該デフォルトルートを使用して転送するトラヒック量が第1のいき値を超えたときに、該ルートの終点となるノード装置との間にダイレクトな暗号トンネルを構築するステップを備えることを特徴とする。

【0025】

#### 【発明の実施の形態】

図2は、本発明の暗号通信を行うネットワークシステムの例を示す図である。図中、端末11から端末31宛に送出された平文パケットは、拠点1のルータ1の入力I/F部に入力される。入力されたパケットはルーティング部を介してヘッダに含まれる宛先IPアドレス（端末31）に基づきルーティング処理され、IPsec処理部に渡される。

【0026】

IPsec処理部では、入力平文パケットの宛先アドレス情報に基づき出力ポリシーデータベース（SPD）およびセキュリティアソシエーションデータベース（SAD）を検索し、終点IPアドレス、転送先アドレス、リンク番号、暗号化の有無、暗号化手段などを決定する。そして、その決定に従ってパケットを中継ノードに送出する。

【0027】

しかしながら、この暗号通信トラヒックが増えてくると、中継ノードでの復号化および暗号化処理の負荷が大きくなっていくので、あるいき値を超えた段階で拠点1（端末11）から拠点2（端末31）へ直接接続する暗号トンネルを構築すると、中継ノードでのパケットの暗号化／復号化負荷の軽減することに効果的である。

【0028】

直接接続する暗号トンネルの構築はDDT（Direct/Default Table）、SAD、SPDを参照して行われる。なお、本実施の態様では、中継ノードにおける復号化／暗号化処理の軽減も意図している。

【0029】

以下、図 1 と図 3 との相違点に着目し説明する。

【 0 0 3 0 】

図 1 によれば、端末 1 1 から端末 3 1 との間で通信が行われているときは、デフォルトルートを選択した場合には、必ず中継ノードを経由し、そこで復号化／暗号化処理が行われる。ここで、デフォルトルートとは、何らかの手段を使って予め設定されている経路を意味する。

【 0 0 3 1 】

しかしながら、図 3 では、端末 1 1 から端末 3 1 との通信が行われているときにルータ 1 とルータ 3 との間に新たな暗号トンネルを設定する。そして、ルータ 1 は暗号通信パケットをデフォルトルートから新たなダイレクトルートへのトンネル切替えを行う。ここで、ダイレクトルートとは、始点となるノード装置（例えばルータ装置）から終点となるノード装置までの経路を意味する。

【 0 0 3 2 】

この暗号トンネルの切替えにより、中継ノードでの暗号化／復号化の処理は行わなくてよくなり、合理的な資源の割り当てが可能になる。

【 0 0 3 3 】

また、中継ノードでの処理負荷を軽減することもできる。なお、新たな暗号トンネル（ダイレクトルート）は、同じデフォルトルートを経由する場合もあれば、異なるルート（経路）を経由する場合もある。

【 0 0 3 4 】

次に、図 2 に示した本発明に関する SPD、DDT、SAD について、それぞれデータ構造の設定例を説明する。

【 0 0 3 5 】

SPD は、拠点間での暗号通信に関するセキュリティポリシーに関する情報を格納する。図 4 は、図 2 に記載の SPD (Security Policy Database) の例を示すものである。

【 0 0 3 6 】

図 4 において、始点 IP アドレスは、拠点 1 が収容するドメインを示す。例えば、端末 1 1 の IP アドレスが 1 0 0 . 1 0 . 1 . 1 2 0 とする。一方、SPD

の始点 I P アドレスが 1 0 0 . 1 0 . 1 . 0 / 2 4 であれば、この始点 I P アドレスの条件に該当することになる。( / 2 4 は I P アドレスの表現の 1 つであり、先頭ビットから 2 4 ビットが一致するアドレスを意味する。つまり、最後の 8 ビットが不一致であっても同じ I P アドレスと見なす表現である。)

終点 I P アドレスは、例えば、端末 1 1 から端末 3 1 に向けてパケットを送出した場合、端末 3 1 への送信先アドレスが終点 I P アドレスに該当する。

#### 【 0 0 3 7 】

例えば、図 4 のにおいて、例えば、始点アドレスが 1 0 0 . 1 0 . 1 . 1 1 で終点アドレスが 1 0 0 . 1 0 . 3 . 3 1 のパケットは、図 4 の第一行目のポリシーデータに沿って I P パケットが処理される。即ち、出力リンク番号は 1、暗号化、対象プロトコルは何でも可である。更に、転送ルートはデフォルトルート（中継ノードであるルータ 2 を経由する）が採用される（図 3）。なお、ルータ 2 は複数存在してよく、また、複数の経路を形成してもよい。

#### 【 0 0 3 8 】

以上のように、S P D の役割は、始点 I P アドレス、終点 I P アドレスに基づき、適用対象となるポリシー情報を取り出し、暗号化 / 非暗号化 / 破棄のいずれかを決定するとともに、リンク番号を選択し、デフォルトルート / ダイレクトルートのいずれかを保持する。

#### 【 0 0 3 9 】

図 5 は、DDT ( D i r e c t / D e f a u l t T a b l e ) の例を示す図である。

#### 【 0 0 4 0 】

図中、宛先 I P アドレスはパケットの転送先拠点アドレスを示す。例えば、ドメインに割り当てられた I P アドレス、あるいは端末の I P アドレスであってもよい。

#### 【 0 0 4 1 】

転送先 I P アドレスはパケットの転送先 I P アドレスを示す。

#### 【 0 0 4 2 】

例えば、転送先 I P アドレスはパケットを転送する次のルータの I P アドレス

であってもよく、ドメインに割り当てられたIPアドレスであってよい。

【0043】

図6は、SAD (Security Association Database) の例を示す図である。

【0044】

終点IPアドレスはルータ装置のインタフェースカードに割り当てられたものであってもよい。

【0045】

図中、外部ヘッダの終点IPアドレスはカプセル化したパケットの終点IPアドレスを示している。

【0046】

また、リンク番号は、ルータ装置内のルーティング部が選択するリンク番号である。IPsecプロトコル種別は、暗号通信を行うためのプロトコルを指定する。ここでは、ESP (Encapsulating Security Payload) を選択するものとする。

【0047】

SPI (Security Parameter Index) はSA (Security Association) を識別するために使用される。Direct表示は、現在の暗号通信が中継ノードを経由し、少なくとも2本のトンネルを介して暗号通信(Defaultルート)が行われているのか、あるいは1本のトンネルを介して暗号通信(Directルート)が行われているのかを表示する。

【0048】

図7は、図2に記載のルータ1のIPsec処理部において、暗号化対象パケットを受信した場合の処理フローを示す図である。

【0049】

ステップJ1では、暗号化対象パケットを受信すると、この受信パケットから送信先アドレスおよび送信元アドレスを抽出する。そして、送信先アドレスおよび送信元アドレスをキーにしてSPDを検索する。例えば、送信先アドレスが100.10.3.31、送信元アドレスが100.10.1.11であった場合

、図4に示すSPDを検索すると、リンク番号は”1”、ポリシーは”暗号化”、プロトコルは”any”、Direct Flagは”Default”が得られる。

【0050】

したがって、リンク情報が”1”と設定されているので、ステップJ2に分岐する。しかしながら、このリンク情報が設定されていない場合には、ステップS1に分岐する。このケースを想定し、ステップS1での処理を説明する。

【0051】

ステップS1では、暗号トンネルに関する設定情報がないので、中継ノードまでの暗号トンネルを構築するとともにSPD、SAD、及びDDTにその情報を設定する。そして、ステップS9に分岐する。

【0052】

なお、暗号トンネルを構築するまでは、受信パケットは一次的にバッファ等に蓄積される。

【0053】

また、設定例については、図4乃至図6を参照されたい。なお、中継ノードから終端の拠点までは暗号化トンネルが前以って何らかの手段（例えば手動でもよい）により設定されているものとする。

【0054】

なお、defaultルートは、前以って暗号化トンネルを静的に構築しておくことが望ましい。

【0055】

ステップJ2では、既にリンク情報が設定されているので、受信パケット対応するDirect Flag情報を参照する。

【0056】

このFlag情報がDefaultルート（中継ノードを介して2つ以上の暗号トンネルを経由）であれば、ステップJ3に進む。そうでなければ（Directルート）、ステップS7に進む。

【0057】

ステップJ3では、Direct接続のトンネル設定が起動要求済かどうかを判定する。すなわち、受信パケットの送信元アドレスおよび送信先アドレスを用いてDDTを検索し、受信パケットに対応する起動要求フラッグを調べる。この値が“On”であればトンネル設定要求済と判定し、ステップS5に進む。そうでなければ、この値は“Off”としてステップS2に進む。

【0058】

ステップS2では、暗号トンネルの始点となる拠点から終点となる拠点までの間に1本のトンネル(Directトンネル)を構築する。そして、同時に、SAD、SPD、DDTに暗号トンネル情報を設定する。

【0059】

ステップS3では、前記暗号トンネルについて、DDTの対応する箇所の起動要求Flagを“On”に書き換える。

【0060】

ステップS4では、SPD、SADに従って、Defaultルートを選択する。そして、ステップS9に分岐する。

【0061】

ステップS5は、ステップJ3の判定処理において、DDTに起動要求Flagに“On”になっているときに、ここに分岐してくる。ここでは、SPD、SADに従ってDefaultルートを選択する。そして、defaultルートを経由する受信パケットの単位時間当たりのトラヒック量を計算する。この計算にはパケット数をカウントするとともに単位時間あたりのトラヒック量も算出する。そして、ステップS9に進む。

【0062】

ステップS7は、ステップJ2の判定処理において、SPDにDirectFlagに“Direct”が設定されているときに、ここに分岐してくる。受信パケットの送信先として、SPD、SADに従いDirectルートを選択する。そして、Directルートを経由する受信パケットの単位時間当たりのトラヒックを計測する。そして、ステップS9に進む。

【0063】

ステップJ1において、リンク情報が設定されていない場合は、ステップS1に分岐する。

#### 【0064】

ステップS1では、暗号化パケット通信に関する制御情報等をSADに設定する。また、Direct Flagフィールドに"Default"を設定し、リンク情報も設定する。そして、ステップS9に進む。

#### 【0065】

ステップS9では、受信パケットを所望のリンクに出力する。

図8は、図7記載のステップS2、S3の詳細処理の説明である。

図中、ステップS21～23は、図7でのステップS2～S3に対応する。まず、ステップS2において、ダイレクトトンネル設定要求を要求すると、ステップSS21が起動される。ステップS22では、受信パケットに対応するDDTの始点IPアドレスおよび終点IPアドレスに基づき、対応するDDT上の設定情報を特定する。

#### 【0066】

次に特定した設定情報に基づきSA（トンネル）情報を生成し、SADにトンネルに関する情報を設定する。そして、ダイレクトトンネルの構築を行う。

#### 【0067】

トンネルの構築手順の例を図7の中程に示す。この例では、Initiator, Responder, Actionに分けて、プロトコルシーケンスを記載している。シーケンスはSA確立要求から認証応答、およびINITIAL-CONTACTまでの手順を記載している。

#### 【0068】

ステップS23では、現在、受信パケットの転送に使用しているDefaultルートからDirectルートへの変更を行う。具体的には、この変更はSPDのリンク番号を上書きすること、および、種別フィールドの値をDirectに変更することによりDirectトンネルを介した暗号通信を行うことができる。

#### 【0069】



以上、ステップS21～S23が図7のステップS2～S3に対応する。

図9は、トラヒック監視処理の処理フローを説明する図である。図7記載のステップS6、S8は、それぞれDefaultルートおよびDirectルートを經由する単位時間当たりのパケット量（トラヒック）をカウントする。このカウントした値は、図9に示すトラヒック監視部により監視される。このトラヒック監視部はIPsec処理部の中にある。

【0070】

図中、ステップS31は、予め設定された時間間隔で単位時間当たりのトラヒックを測定するために起動される。

【0071】

ステップJ31では、起動されたトラヒック監視部は、SADを参照し、各現在の処理ルートが暗号化処理を行うリンク番号に対応して、DefaultルートかDirectルートかを判定する。"Default"ならば、ステップJ33に分岐し、"Direct"ならばステップJ32に分岐する。

【0072】

ステップJ32では、単位時間当たりのDirectルート使用パケット数が域値以上であれば、継続してDirectルートを使用するとともにステップS8でパケットをカウントするカウンタをゼロクリアする。そして、ステップJ34に分岐する。

【0073】

ステップS32、S34では、ダイレクトルートの使用を解除する要求を行う。そして、ステップS8でパケットをカウントするカウンタをゼロクリアする。そして、ステップJ34に分岐する。（詳細は後述）。

【0074】

ステップJ33では、単位時間当たりのDefaultルート使用パケット数が域値以上であれば継続してDefaultルートを使用するとともにステップS6でパケットをカウントするカウンタをゼロクリアする。そして、ステップJ34に分岐する。

【0075】

ステップS35, S37では、Defaultルートの使用を解除する要求を行う。なお、予めデフォルトルートを継続的に設定している場合には、動的な解除は不要である。そして、ステップS6でパケットをカウントするカウンタをゼロクリアする。そして、ステップJ34に分岐する。

【0076】

ステップJ34では、SADを参照し、全ての暗号化トンネルについて処理を行ったかどうかを確認する。すべての処理が完了したならば、処理を終了する

図10は図9のステップS32およびS35からトンネル設定解除の処理フローを示す図である。

【0077】

図中、ステップS41では、ダイレクトトンネルの設定解除要求を受付を行う。このとき、パラメータとして、解除するトンネルに関する情報としてSPDから処理の対象とする宛先アドレスを取得する。

【0078】

ステップS42では、取得した宛先アドレスをキーとしてSPDを検索し、解除の対象となるDirectトンネルを特定する。そして、DirectトンネルをDefaultルートに、DeirectをDefaultに修正する。図10のSPD更新経緯を参照。

【0079】

ステップS43は、解除の対象となるDirectトンネルで同一リンクがない場合、つまり、Directトンネルが単独で使用されている場合は、そのトンネルに関する情報をSADから削除する。図10のSAD更新経緯を参照。

【0080】

そして、100.10.3.0/24について、DDTの識別をDirectからDefaultに修正するとともに、起動要求も"On"から"Off"に修正する。

【0081】

ステップS44では、トンネル切断後の接続先へ通知し、セッションを切断する。そして、INITIAL-CONTACTを送信することによりトンネルに関する

る S A を開放する。

【 0 0 8 2 】

本発明の次に示す付記のように構成することもできる。

(付記 1)

1 つ以上のノード装置との間に第 1 の暗号トンネルをそれぞれ設定可能なノード装置において、

パケットを受信し、予め設定された暗号トンネルを介した経路にパケットを送出する手段と、

該経路を使用するパケットのトラフィック量が第 1 のいき値を超えたときに、該経路の終点となるノード装置との間に第 2 の暗号トンネルを構築する手段を備えることを特徴とするノード装置。

【 0 0 8 3 】

(付記 2)

付記 1 記載において、

前記第 2 の暗号トンネルのトラフィック量が第 2 のいき値を下回ったときに、前記第 2 の暗号トンネルから前記第 1 の暗号トンネルに切り換えることを特徴とするノード装置。

【 0 0 8 4 】

(付記 3)

付記 1 記載において、

前記第 1 の暗号トンネルから前記第 2 の暗号トンネルに切り換える処理を行うための切替え要求を示す情報を含む手段を備えることを特徴とするノード装置。

【 0 0 8 5 】

(付記 4)

付記 1 記載において、

セキュリティアソシエーションデータベースを備え、

該セキュリティアソシエーションデータベースは、前記暗号トンネルに対応して、ダイレクトあるいはデフォルトのいずれかを示すことを特徴とするノード装置。

(付記 5)

付記 1 記載において、

前記第 1 の暗号トンネルをそれぞれ接続する前記すくなくとも 1 つのノード装置および前記経路の終点となるノード装置を有することを特徴とする暗号通信システム。

【 0 0 8 6 】

(付記 6)

パケットを受信し、第 1 の経路に暗号化したパケットを送出するステップと

、  
該第 1 の経路を使用して転送するパケットのトラフィック量が第 1 のいき値を超えたときに、前記経路の終点となるノード装置との間に暗号トンネルを構築するステップを備えることを特徴とする暗号通信を行う方法。

【 0 0 8 7 】

【発明の効果】

本発明によれば、暗号通信に使用されるトンネルに関するリソースを合理的に割り当てることが可能になる。

【図面の簡単な説明】

【図 1】 従来の暗号通信におけるデフォルトネットワークを示す図である。

【図 2】 本発明に係るネットワークにおけるルータ装置の構成の例を示す図である。

【図 3】 本発明に係るデフォルトルートとダイレクトルートの切替えの例を示す図である。

【図 4】 本発明に係る Security Policy Database の設定例を示す図である。

【図 5】 本発明に係る Default / Direct Table の設定例を示す図である。

【図 6】 本発明に係る Security Association Database の設定例を示す図である。

【図 7】 本発明に係るルータ装置の I P s e c 処理部の処理フローを示す図である。

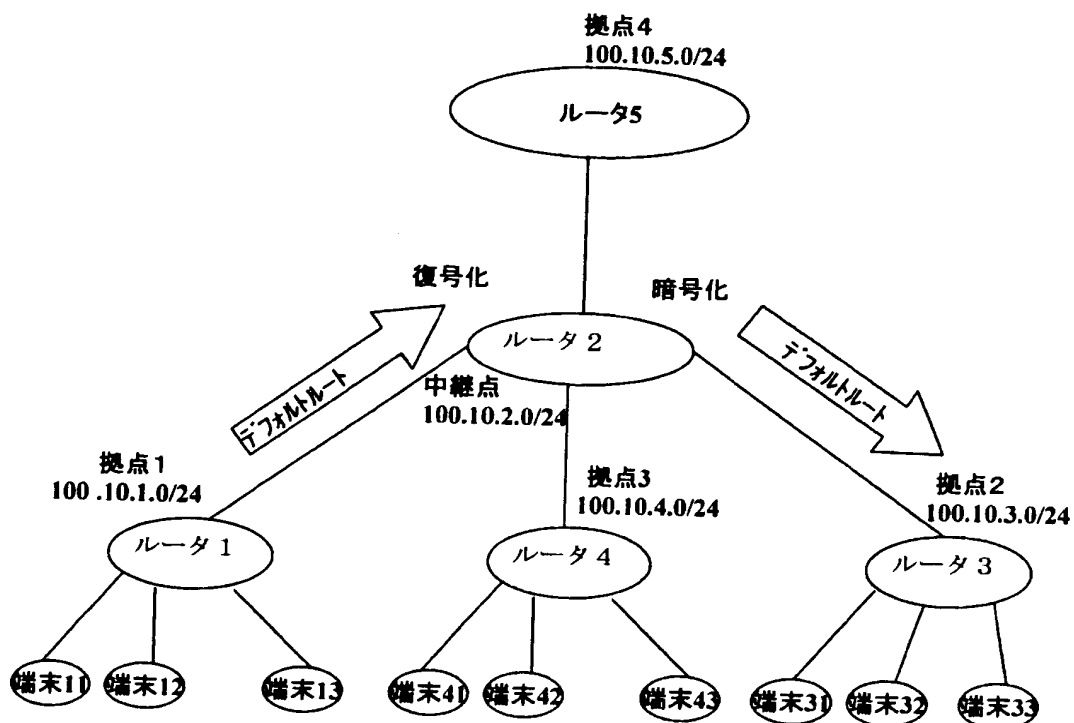
【図 8】 本発明に係る図 7 記載のステップ S 2 および S 3 の処理フローを説明する図である。

【図 9】 本発明に係るトラヒック監視部の処理フローを示す図である。

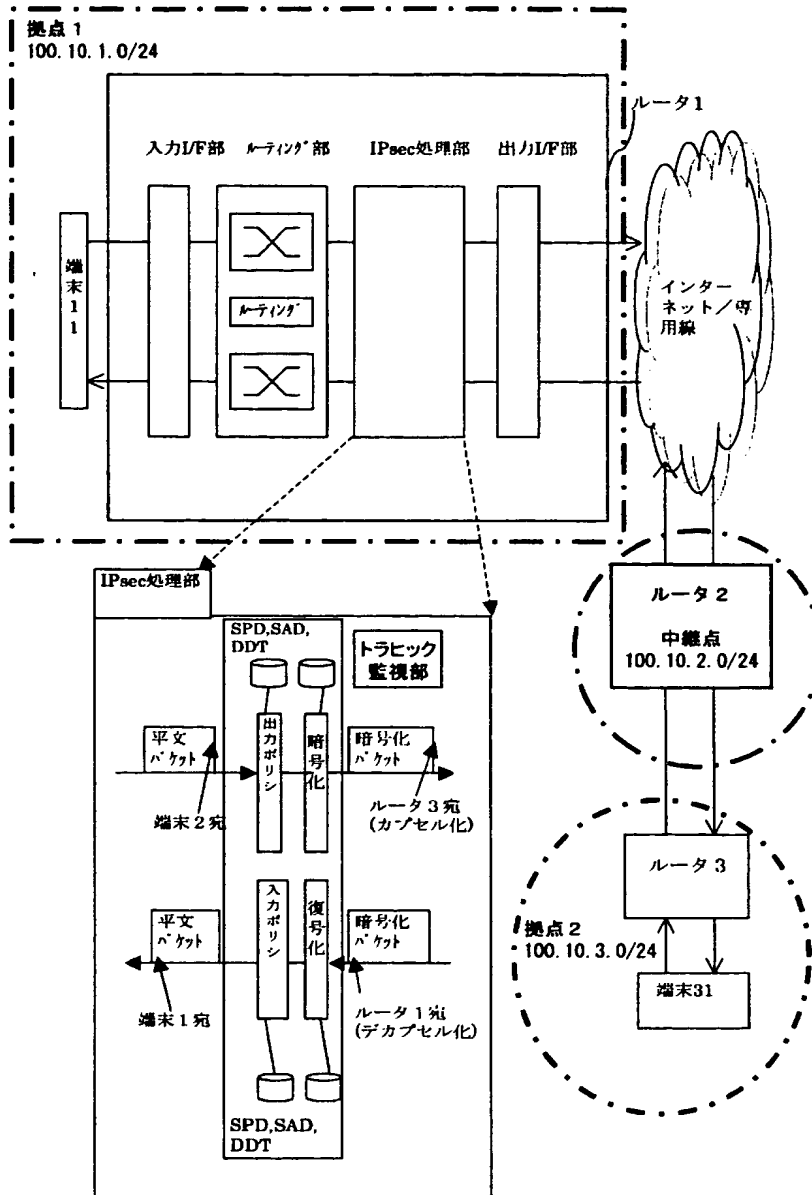
【図 1 0】 本発明に係る D i r e c t トンネルを解除する処理フローを示す図である。

【書類名】 図面

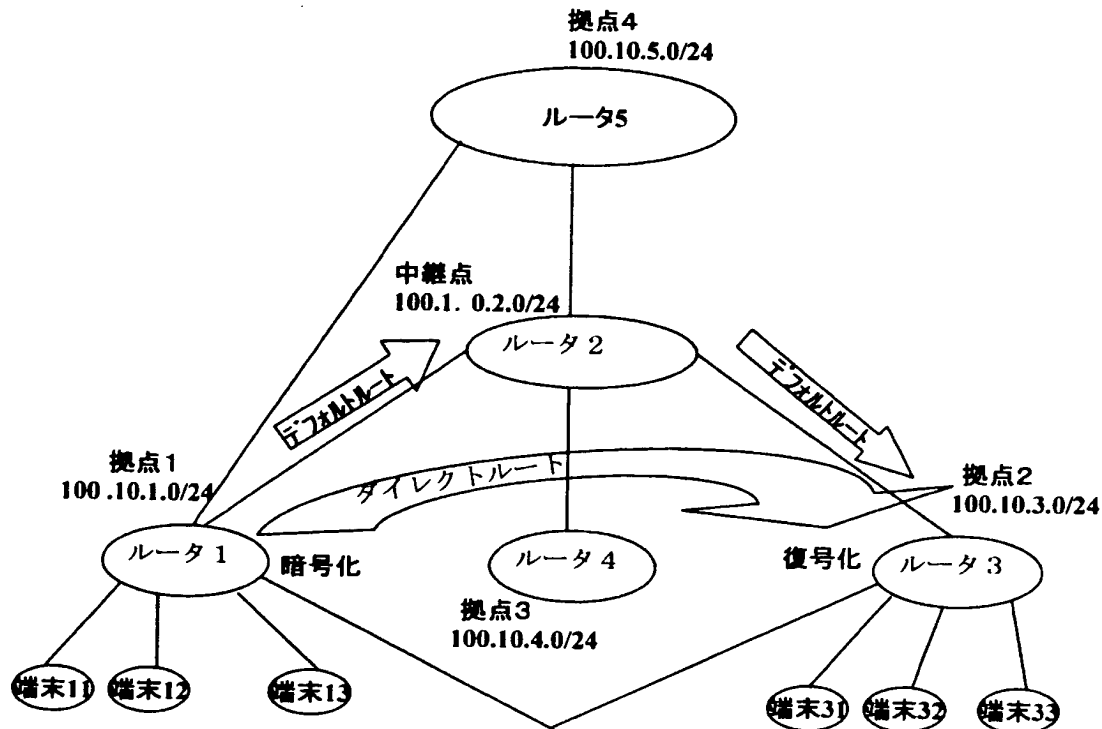
【図 1】



【図 2】



【図 3】



【図 4】

S P D (Security Policy Database) の設定例

始点IPアドレス	終点IPアドレス	リンク番号	ポリシー	プロトコル	Direct Flag
100.10.1.0/24	100.10.3.0/24	1	暗号化	any	Default
100.10.1.0/24	100.10.3.0/24	2	暗号化	any	Direct
100.10.1.0/24	100.10.5.0/24	3	非暗号化		
100.10.1.0/24	100.10.6.0/24		破棄		



【図 5】

DDT (Default/Direct Table)

宛先IPアドレス	転送先IPアドレス	ホリシ	識別フラグ	起動要求	.....
100.10.3.0/24	100.10.3.0/24	暗号化	Default		
100.10.4.0/24	100.10.4.0/24	暗号化	Direct	Off	

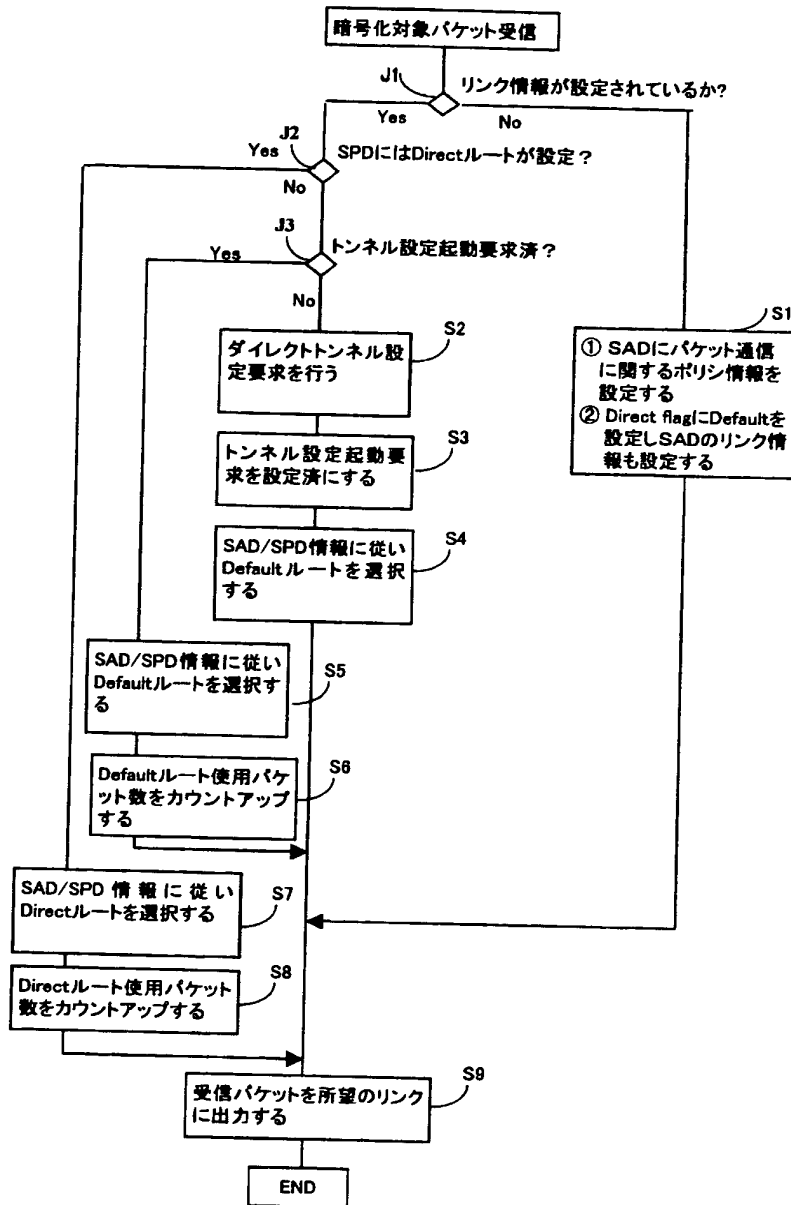
【図 6】

SAD (Security Association Database)の例

外部ヘッダの 終点IPアドレス	リンク 番号	IPsecプロト コル種別	SPI値	その他SA パラメタ	Direct 表示
100.10.2.1	1	ESP	0x32e9a7c6	....	Default
100.10.3.1	2	ESP	0x32e9a7c8	....	Direct
100.10.5.1	3				
100.10.6.1					

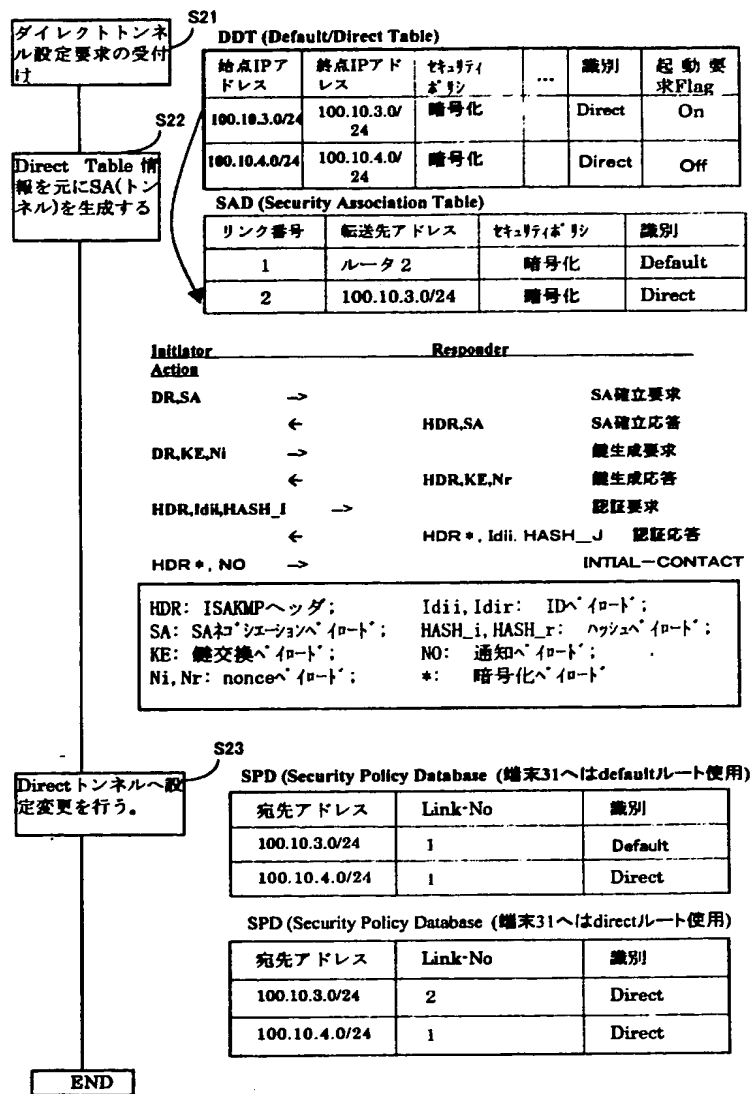
SPI: Security Parameter Index  
ESP: Encapsulating Security Payload

【図 7】

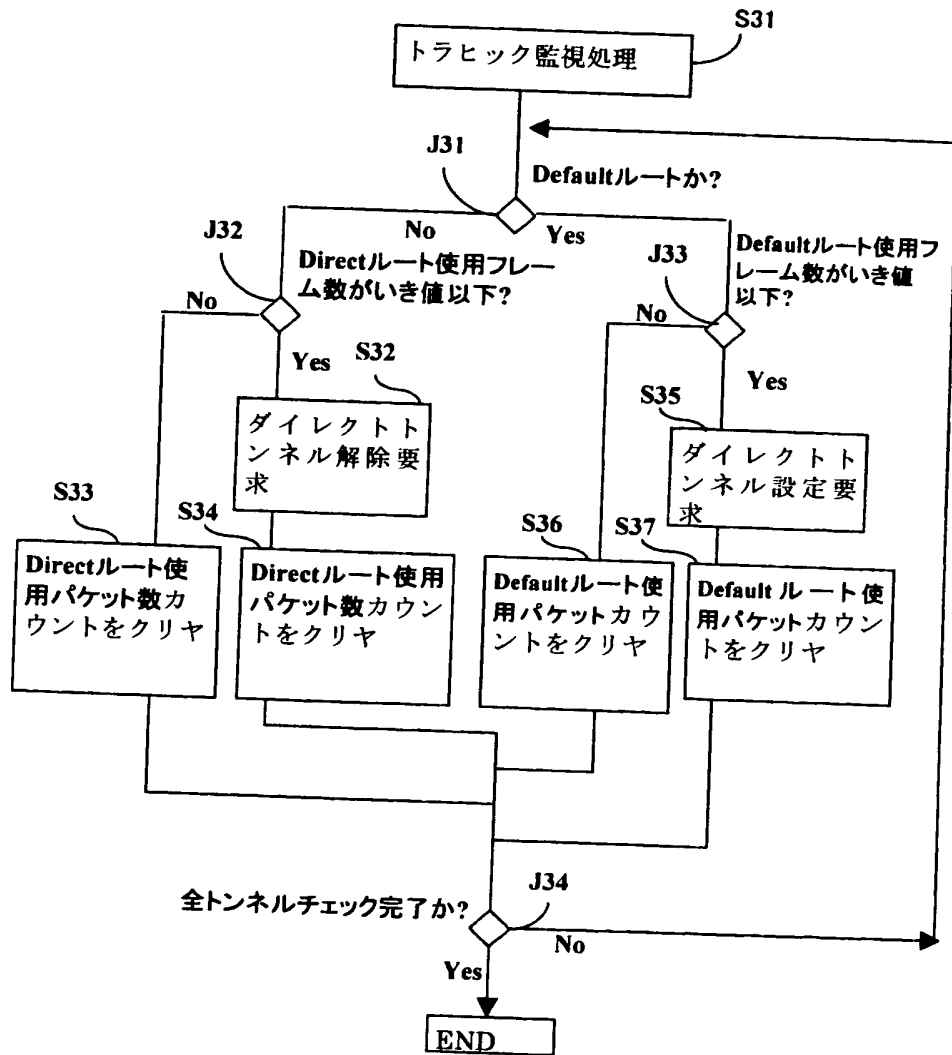


【図 8】

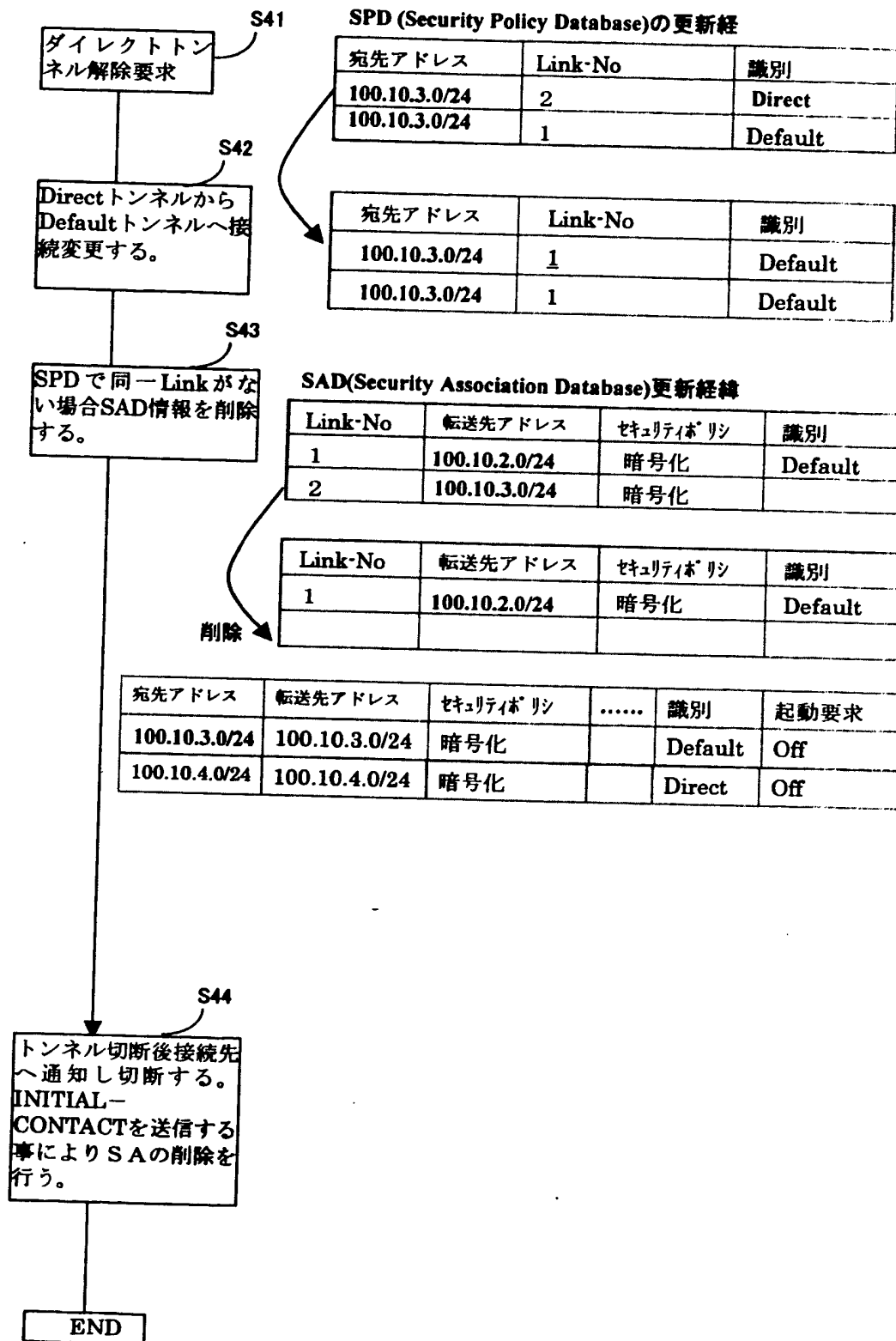
図7記載のステップS2およびS3の詳細説明



【図 9】



【図10】



【書類名】 要約書

【要約】

【課題】

暗号通信に使用されるトンネルに関するリソースを合理的に割り当てることを目的とする。

【解決手段】

ノード装置 1 と接続可能な 1 つ以上の中継ノード装置 2 との間にデフォルトの暗号トンネルをそれぞれ設定し、ノード装置 1 は IP パケットを受信しデフォルトルートに暗号化パケット転送する。その後、該デフォルトルートを使用して転送するパケットの量が第 1 の域値を超えたときに終点となるノード装置との間にダイレクトな暗号トンネルを構築し、そのダイレクトなルートに IP パケット転送を切り換える。

【選択図】 図 3

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 5 2 2 3 ]

1. 変更年月日	1 9 9 6 年 3 月 2 6 日
[ 変更理由 ]	住所変更
住 所	神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号
氏 名	富士通株式会社